(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 881 596**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **05 50254**

(51) Int Cl[8] : **H 04 L 12/22** (2006.01), H 04 L 9/30

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.01.05.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.08.06 Bulletin 06/31.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *THOMSON LICENSING S.A. Société anonyme* — FR.

(72) **Inventeur(s) :** ANDREAUX JEAN PIERRE, DURAND ALAIN et LELIEVRE SYLVAIN.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** THOMSON.

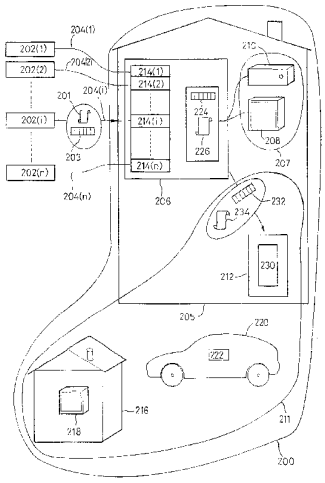
(54) PROCEDE DE PROTECTION DE CONTENUS NUMERIQUES AUDIO ET/OU VIDEO ET DISPOSITIFS ELECTRONIQUES METTANT EN OEUVRE CE PROCEDE.

(57) Cette invention concerne un procédé de protection d'un contenu (201) fournisseur audio et/ou vidéo d'un fournisseur (202(i)) dans un domaine (200) client comprenant un dispositif (212) isolé portable.

Conformément à cette invention, un tel procédé de protection est caractérisé en ce que:

a. le dispositif (212) isolé portable reçoit un contenu (232) isolé, résultat d'un traitement nurnérique du contenu (201) fournisseur audio et/ou vidéo, et une licence (234) isolée associée au contenu et contenant des droits d'utilisation du contenu (232) isolé et des informations d'autorisation,

b. le dispositif (212) isolé portable gère la consommation du contenu (232) conformément aux droits associés qu'il a reçu dans des dispositifs du domaine (200), indépendamment du fournisseur (202(i)).



FR 2 881 596 - A1

PROCEDE DE PROTECTION DE CONTENUS NUMERIQUES AUDIO ET/OU VIDEO ET DISPOSITIFS ELECTRONIQUES METTANT EN ŒUVRE CE PROCEDE.

La présente invention se rapporte à un procédé de protection de contenus numériques audio et/ou vidéo et à des dispositifs électroniques mettant en oeuvre ce procédé, notamment dans le cadre d'un domaine client de dispositifs de traitements de contenus numériques.

Des producteurs de contenus numériques (par exemple et sans limitation films, documentaires, musiques, clips, jeux vidéos, contenus audiovisuels, services ou autres, ...), afin de contrôler la consommation de leur production distribuée par des réseaux numériques comme Internet et d'éviter le piratage, mettent en œuvre des procédés de gestion de droits de consommation associés aux contenus cédés à leurs clients. Ces procédés sont dénommés par la suite procédés DRM (initiales en anglais de « Digital Right Management » signifiant « Gestion de Droits Numérique »).

Les droits associés à un contenu peuvent autoriser par exemple la reproduction du contenu pendant un certain nombre d'heure et/ou un certain nombre de fois et/ou la réalisation d'un certain nombre de copies. Il faut alors faire le suivi des droits au fur et à mesure de la consommation des contenus par les clients.

Des moyens de mise en œuvre d'un procédé DRM existent du côté fournisseur, sous la forme d'un module logiciel appelé DRM fournisseur, et du côté client, sous la forme d'un module logiciel dénommé DRM client.

Souvent, la consommation des contenus se réalise au niveau d'un dispositif électronique, dénommé dispositif d'accès, par exemple un ordinateur, connecté à un réseau délivrant les contenus, dénommé réseau fournisseur, et ce dispositif contient un ou des module(s) DRM client.

Il se peut que les contenus soient stockés ou consommés sur d'autres dispositifs du client, qui ne soient pas directement connectés au réseau fournisseur.

Pour éviter la propagation incontrôlée des contenus, la diffusion de ces contenus peut être restreinte à un ensemble de dispositifs de traitement de contenus, généralement appartenant à un même client (par exemple télévisions, consoles de jeux, radios, appareils reproducteurs de musiques, décodeurs,...).

Cet ensemble de dispositifs associés à un client est dénommé domaine client dont la figure 1 montre un exemple.

Un fournisseur 102 (i) , 1<=i<=n, de contenus vidéo et/ou audio fournit un contenu 103 numérisé (notamment embrouillé ou en clair), dénommé contenu 103 fournisseur, et des droits, dénommés droits fournisseur, associés au contenu 103 fournisseur et contenus dans une licence 101 fournisseur. Cette fourniture se produit par des réseaux 104(i) fournisseurs, 1<=i<=n, connectés à un dispositif 106 d'accès d'un domaine 100 client.

Les réseaux 104(i) peuvent notamment appartenir au fournisseur ou être publics, comme par exemple Internet.

Il existe entre chaque fournisseur 102(i) et le dispositif 106 d'accès un procédé DRM.

Des procédés de protection des droits ont été développés pour protéger les droits fournisseur dans le domaine 100, et contrôler que la consommation d'un contenu se réalise légitimement :

- au niveau du dispositif 106 d'accès ou
- au niveau d'une partie des dispositifs électroniques, dénommée partie 107 réseau, comprenant par exemple un téléviseur 108 ou un appareil reproducteur 110 de musique, connectés en réseau au dispositif 106 d'accès, notamment par un câble coaxial, une fibre optique ou par des systèmes de communications sans fils. Ces dispositifs sont dénommés dispositifs reliés.

En effet, le contrôle de la consommation de contenus nécessite généralement une connexion à un module 114(i) DRM client pour vérifier les autorisations de consommation, opération qui peut se réaliser plusieurs fois lors de la consommation d'un contenu.

La création et la gestion d'un domaine 100 comprenant seulement un dispositif 106 d'accès et une partie 107 réseau ont été décrites dans le document WO 00/62505 A1 intitulé "Digital Home Network and method for creating and updating such a network".

Plus précisément, le document EP 1 253 762 A1 intitulé "Process for managing a symmetric key in a communication network and devices for the implementation of this process" définit un procédé de gestion où les contenus sont chiffrés et déchiffrés grâce à une clé symétrique que connaissent notamment le dispositif 106 et les dispositifs de consommation de la partie 107 réseau.

Un cas particulier de droits (droits de seule consommation sans droits de copies, dénommés en anglais droits « view-only ») est traité dans le document WO 02/47356 A2 intitulé "Method of secure transmission of digital data from a source to a receiver".

L'invention résulte de la constatation que les procédés DRM et procédés de protection de contenus de l'art antérieur ne permettent pas actuellement de gérer de façon sécurisée un contenu et les droits associés à ce contenu, acquis pour un domaine 100 à travers un dispositif 106 d'accès, dans des dispositifs de consommation de contenus, dénommés dispositifs isolés, inclus dans une partie 111 dénommée partie isolée du domaine 100, sans introduire de module DRM complets différents, dépendant chacun d'un fournisseur (i) potentiellement utilisable, dans les dispositifs isolés. Les dispositifs isolés sont par exemple:

- un dispositif 112 portable, par exemple un baladeur audio et/ou vidéo, permettant de consommer un contenu là où le client le souhaite; ces types de dispositifs isolés, dénommés dispositifs isolés portables, comme le dispositif 112, peuvent être connectés au dispositif 106 d'accès de façon temporaire pour charger des contenus et des droits,

un dispositif 118 se trouvant dans un site 116, différent du site 105 où est le dispositif 106 d'accès (par exemple une télévision dans une maison secondaire)

ou un dispositif 122 embarqué dans un véhicule 120 de transport ; ces types de dispositifs isolés, dénommés dispositifs isolés distants comme les dispositifs 122 et 118, ne peuvent se connecter au dispositif 106 d'accès.

En effet, ces dispositifs isolés ne peuvent pas établir une connexion réseau avec un module 114(i) DRM client pour obtenir les autorisations nécessaires lors de la consommation d'un contenu.

Or l'introduction de modules DRM complets différents, car dépendants du fournisseur(i), dans les dispositifs isolés entraîne de nombreuses difficultés comme par exemple :

- de nombreux dispositifs isolés n'ont pas des moyens de traitement de l'information suffisants pour contenir plusieurs modules DRM(i) différents,
- il faudrait une liste close et définitive de tous les moyens DRM à introduire, ce qui serait un frein à la concurrence,
- il faudrait que chacune de ces technologies soient figées car elles ne pourraient pas être mises à jour,
- il y aurait également des problèmes de sécurité étant donné que tous les secrets de ces modules DRM seraient réunis sur un seul dispositif isolé.

La présente invention vise donc à résoudre le problème qui consiste à s'assurer que des droits autorisés pour un contenu soient respectés par le client sur l'ensemble de son domaine et notamment au niveau de la partie 111 isolée.

L'invention concerne un procédé de protection d'un contenu fournisseur audio et/ou vidéo d'un fournisseur dans un domaine client comprenant un dispositif isolé portable, caractérisé en ce que:

a. le dispositif isolé portable reçoit un contenu isolé, résultat d'un traitement numérique du contenu fournisseur audio et/ou vidéo, et une licence isolée associée au contenu et contenant des droits d'utilisation du contenu isolé et des informations d'autorisation,
b. le dispositif isolé portable gère la consommation du contenu conformément aux droits associés qu'il a reçu

dans des dispositifs du domaine, indépendamment du fournisseur.

Grâce à cette invention, la gestion des droits dans la partie isolée ne suppose pas l'introduction de modules DRM différents, dépendants chacun d'un fournisseur différent potentiellement utilisable, dans des dispositifs isolés pour consommer des contenus de différents fournisseurs.

Aussi, une seule licence provenant d'un fournisseur, associée à un contenu, est nécessaire, indépendamment du dispositif du domaine utilisé pour consommer le contenu . Cette licence est traitée par le module DRM client.

Un autre avantage est la compatibilité du procédé de l'invention avec les procédés précédents mettant en œuvre une protection de contenu au niveau d'un domaine comprenant un dispositif d'accès et une partie réseau (procédés décrits dans les documents WO 00/62505 A1, EP 1 253 762 A1 et WO 02/47356 A2 cité précédemment). Ainsi le procédé de l'invention peut être utilisé seul ou de façon complémentaire (à partir du dispositif isolé portable) à ces procédés existants.

Un autre avantage de l'invention est le fait qu'un contenu qui a été traité pour être consommé à partir du dispositif isolé portable n'a pas à être re-traité si de nouveaux droits sont acquis pour ce même contenu pour être à nouveau consommé à partir du dispositif isolé portable.

Enfin, cette solution de protection est valable pour tous les dispositifs du domaine client pouvant se connecter momentanément au dispositif isolé portable. Ceci implique que des contenus sont consommables, avec un seul procédé de protection global, sur l'ensemble des dispositifs de consommation pouvant être dans un domaine sans avoir de procédés de protection spécifiques dédiés à des dispositifs particuliers du domaine.

Dans une réalisation, le dispositif isolé portable se connecte à un dispositif d'accès temporairement en vue d'acquérir le contenu isolé et la licence isolée contenant les droits d'utilisation du contenu isolé et les informations d'autorisation.

Dans une réalisation, le dispositif d'accès crée un paquet de données de gestion des droits d'utilisation du contenu, dénommé TEMM, contenant notamment le résultat d'un chiffrement, déchiffrable par le dispositif isolé portable:

- de données d'autorisation,

- d'un identifiant de contenu,
- de droits d'utilisation du contenu,

et envoie ce paquet TEMM au dispositif isolé portable.

Selon une réalisation, le dispositif d'accès crée des paquets de données de contrôle, dénommés TECM, qui sont envoyés au dispositif isolé portable introduits dans le contenu isolé et qui contiennent :

- un ensemble chiffré de données comprenant :
  - une clé d'embrouillage des paquets de données formant le contenu, et
  - des données d'autorisation, et

des informations sur le chiffrement permettant au dispositif isolé portable de déchiffrer l'ensemble de façon sécurisée.

Préférentiellement, la clé d'embrouillage contenue dans le paquet de données de contrôle est en outre protégée par une donnée d'autorisation.

Dans une réalisation, les droits associés au contenu fournisseur dans le dispositif d'accès sont mis à jour en soustrayant les droits envoyés au dispositif isolé portable.

Selon une réalisation, le contenu est consommé au niveau du dispositif isolé portable.

Dans une réalisation, les moyens de gestion envoient l'autorisation de consommation aux moyens de consommation propres au dispositif isolé portable et mettent à jour les droits compris dans la licence isolée au fur et à mesure de la consommation du contenu dans le dispositif isolé portable.

Selon une réalisation, un dispositif ayant des moyens de consommation de contenus, dénommé dispositif de présentation, se connecte au dispositif isolé portable temporairement.

Dans une réalisation, lorsque le dispositif de présentation demande l'autorisation d'acquérir le contenu pour le consommer au dispositif isolé portable, les moyens de gestion du dispositif isolé portable vérifient la présence des droits demandés par le dispositif de présentation dans la licence isolée et, si la demande d'autorisation est justifiée, la mettent à jour et envoient l'autorisation et le contenu au dispositif de présentation pour y être consommé.

Dans une réalisation, le dispositif de présentation appartient au domaine client.

L'invention concerne aussi un dispositif isolé portable.

Conformément à cette invention, un tel dispositif isolé portable contient des moyens de gestion pour mettre en œuvre le procédé selon l'une des réalisations précédentes.

L'invention concerne aussi un dispositif d'accès.

Conformément à cette invention, un tel dispositif d'accès comprend des moyens pour mettre en œuvre le procédé selon l'une des réalisations de procédé de protection précédentes.

D'autres caractéristiques et avantages de l'invention apparaîtront avec la description effectuée ci-dessous à titre d'exemple non limitatif en se référant aux figures ci-jointes sur lesquelles:

- La figure 1, déjà décrite, représente un exemple d'un domaine 100 de dispositifs conforme à l'art antérieur,
- La figure 2 représente schématiquement une réalisation de l'invention dans un domaine client,
- La figure 3 est une description schématique du procédé de transfert d'un contenu entre un module DRM client et un dispositif isolé portable,
- La figure 4 est une représentation schématique de la structure de certaines données, selon un certain standard, lors d'un transfert entre un module DRM client et un dispositif portable.

L'invention permet de gérer les droits de consommation des contenus acquis par un client sur l'ensemble de son domaine, le domaine pouvant inclure des dispositifs isolés portables et des dispositifs isolés distants.

Un exemple de réalisation de cette invention est représenté schématiquement par la figure 2.

Un client a un ensemble, dénommé domaine 200, de dispositifs électroniques de traitement de contenus numériques audio et/ou vidéo.

Le client du domaine 200 passe une commande d'un contenu avec des droits associés à un fournisseur 202(i), 1<=i<=n, de contenus grâce à des moyens 214(i), 1<=i<=n, de gestion des droits, dénommés modules 214(i) DRM client, intégrés dans un dispositif 206 d'accès.

Le dispositif 206 d'accès reçoit alors grâce à un réseau 204(i) , 1<=i<=n, comme par exemple Internet ou un réseau câblé, un contenu

fournisseur 203 audio et/ou vidéo et une licence fournisseur 201 de consommation. Le contenu 203 est fourni le plus souvent sous la forme de paquets de données audio/vidéo (ou autre données) protégés par le DRM fournisseur, par exemple en étant chiffrés ou embrouillés à l'aide d'une clé du fournisseur.

La licence fournisseur 201 contient quant à elle des droits de consommation associés au contenu 203, des données permettant d'accéder au contenu (par exemple, la clé du fournisseur utilisée pour chiffrer des paquets de données du contenu) ainsi qu'un identifiant du contenu. Le tout est protégé, par exemple en étant chiffré, de manière à ne pouvoir être accessible que par le module 214(i) DRM client associé au fournisseur 202(i) du contenu. La licence 201 est reçue et gérée par le module 214(i) DRM client.

Le contenu 203 et la licence 201 sont alors convertis en contenu propre au domaine 200, dénommé contenu personnalisé 224, et en licence propre au domaine 200, dénommée licence personnalisée 226, dans le dispositif 206 d'accès. Il s'agit notamment d'une adaptation des structures de données au domaine 200. Alors, le client peut choisir de consommer le contenu personnalisé 224 soit directement dans le dispositif 206 d'accès, soit dans une partie 207 réseau (dispositifs 210 ou 208), comme dans l'art antérieur.

En effet, dans une réalisation, cette personnalisation du contenu, sa gestion et sa consommation dans le dispositif 206 d'accès ou dans la partie 207 réseau peut se faire notamment selon l'une des méthodes décrites dans les documents WO 00/62505 A1, EP 1 253 762 A1 ou WO 02/47356 A2 cités précédemment.

Plus précisément, selon ces exemples de réalisation, le contenu reçu 203 est mis en forme (s'il n'est pas déjà dans la forme requise) dans le dispositif d'accès 206 de telle sorte que les paquets de données audio/vidéo ou autre soient embrouillés par des mots de contrôle notés CW (de l'anglais « Control Word »), renouvelés lors de chaque cryptopériode du signal (typiquement toutes les 10 s) pour former le contenu personnalisé 224. Les droits de consommation associés au contenu 203, qui sont inclus dans la licence 201, sont quant à eux convertis selon un format propre au domaine 200. Dans les exemples de réalisation décrits dans les documents mentionnés plus haut, le format des droits propre au domaine contient trois états possible :

- « copie privée » (c'est à dire copie du contenu autorisée mais seulement pour une consommation future dans le domaine 200),
- « copie libre » (copie autorisée sans condition), ou
- « view-only » (c'est à dire autorisation seulement de consommer le contenu sans en réaliser de copie pour une consommation future).

Les droits convertis sont inclus dans des messages notés LECM qui contiennent également les mots de contrôle CW chiffrés par une clé symétrique K_{LECM} et le chiffrement de cette clé K_{LECM} par une clé propre au domaine K_N. Les dispositifs 208, 210 de présentation du contenu à l'utilisateur appartenant au domaine 200 contiennent la clé K_N (stockée dans une mémoire sécurisée) et sont donc capables de retrouver K_{LECM}, puis les mots de contrôle CW de manière à désembrouiller les paquets de données du contenu personnalisé 224.

Les messages LECM, qui correspondent dans cet exemple à la licence personnalisée 226, sont transmis avec les paquets de données du contenu 224, en étant répétés lors de chaque cryptopériode.

On notera que le client peut aussi, grâce à cette invention, consommer le contenu personnalisé 224 (après adaptation éventuelle, il devient alors un contenu 232 isolé) au niveau d'une partie isolée 211 du domaine client 200 comprenant par exemple un dispositif 212 isolé portable et/ou un dispositif 222 dans une voiture 220 et/ou un dispositif 218 dans une maison secondaire 216, ces derniers étant dénommés dispositifs isolés distants.

Le dispositif 212 isolé portable peut contenir des moyens de consommation (par exemple un écran d'affichage et un haut-parleur ou une prise pour un casque) notamment si ce dispositif 212 est un baladeur audio et/ou vidéo ou ne pas les contenir (dans ce cas, ce dispositif peut être notamment un dispositif de stockage et de traitement cryptographique).

Pour cela, le dispositif 212 isolé portable contient un module 230 de gestion des droits, mettant en œuvre un procédé de protection, notamment pour la partie 211 isolée du domaine client 200, dénommé procédé de protection isolé.

Le module 230 est générique (c'est à dire qu'il ne dépend pas du fournisseur du contenu 203), sécurisé (c'est à dire qu'il est résistant à la fraude), et il stocke des données de chiffrement et d'autorisations de consommation.

Le dispositif 212 isolé portable reçoit, quand il se connecte au dispositif 206 d'accès pour acquérir un contenu :

- un contenu 232 isolé, adapté pour être consommé dans le dispositif 212 ou pour être diffusé de manière contrôlée à partir du dispositif 212 isolé,
- et une licence 234 additionnelle, dénommée licence isolée, contenant les droits d'utilisation du contenu que le client veut utiliser à partir du dispositif 212 isolé dans le domaine 200, notamment dans la partie 211 isolée, et les données nécessaires pour autoriser cette utilisation.

Une mise à jour des droits restants dans le dispositif 206 d'accès se réalise en déduisant de la licence fournisseur 201 les droits transmis au dispositif 212 isolé dans la licence 234.

Par exemple, si le client a acquis le droit de voir deux fois un film et qu'il souhaite le voir une fois dans sa maison 216 secondaire, le droit de le voir une fois est transmis au dispositif 212 isolé portable, pour être ensuite transmis, quand cela sera requis, à la télévision 218.

Parallèlement, ce droit transmis est alors décompté des droits présents dans le dispositif 206 d'accès pour ainsi ne plus laisser que le droit de voir le film une seule fois au niveau du dispositif 206 d'accès.

La transmission du contenu 232 et de la licence 234 est sécurisée grâce à un embrouillage/chiffrement de certaines données associées au contenu grâce à des données de chiffrement stockées notamment dans le module 230.

Le module de gestion des droits 230 est, pour cela, inclus dans une carte à puce ou un processeur sécurisé, qui met en œuvre le procédé de protection isolé et contient notamment les clés de chiffrement stockées de manière sécurisée.

L'adaptation du contenu 224 personnalisé et de la licence 226 personnalisée en un contenu 232 isolé et en une licence 234 isolée est donc une étape importante qui doit assurer la sécurité des droits gérés à partir du dispositif 212 isolé portable.

Nous allons maintenant décrire un exemple de réalisation de cette adaptation du contenu personnalisé 224 et de la licence personnalisée 226 en

un contenu isolé 232 et en une licence isolée 234 en liaison avec la figure 3 et la figure 4 (qui apporte des précisions quant à la structure des données).

Selon un mode de réalisation préféré de l'invention, la licence isolée 234 est transmise au dispositif 212 isolé portable sous la forme de deux « objets » :

- d'une part des messages, appelés TECM, qui correspondent aux messages LECM de la licence personnalisée 226 mais dans lesquels la clé de chiffrement symétrique K_{LECM} n'est plus chiffrée avec la clé K_N propre au domaine de l'utilisateur mais avec une clé K_{DP} propre au dispositif 212 isolé portable ;

- d'autre part, dans le cas où les droits associés au contenu sont de type « view-only », un message noté TEMM qui contient des informations d'autorisation permettant de consommer ultérieurement le contenu sur des dispositifs isolés distants 218, 222 du domaine de l'utilisateur.

La figure 3 illustre un protocole de transfert entre :

- le dispositif 302 d'accès, équivalent au dispositif 206 d'accès de la figure 2,
- et le module 304 de gestion (équivalent au module 230 de la figure 2) propre au dispositif 212 isolé portable ;

lorsque les droits associés au contenu à transmettre sont de type « view-only ».

Le module 304 dispose d'un système asymétrique certifié de chiffrement comprenant une clé 306 publique (KpubTr) et une clé 312 privée (KprivTr) en vue de s'identifier auprès du dispositif 302 d'accès.

Le module 304 comprend aussi la clé 314 K_{DP} de chiffrement symétrique propre au dispositif portable.

Lors d'une demande de transfert de contenu entre le dispositif 302 et le module 304, les étapes suivantes sont effectuées:

- étape 350 : le module 304 envoie un certificat 307 comprenant la clé 306 KpubTr au dispositif 302 d'accès,
- étape 352 : le dispositif 302 vérifie la clé 306 KpubTr (et donc l'identité du dispositif 212 portable) grâce à une clé 308 publique, dénommée KpubDRM, qui sert à vérifier le certificat 307 du dispositif 212 portable (si l'identité du dispositif 212 n'est pas reconnue comme valable, alors l'adaptation du contenu et son transfert n'ont pas lieu),

- étape 354 : si la vérification de l'étape 352 est positive, alors le dispositif 302 crée un paquet 340 de données de gestion des droits d'utilisation du contenu, correspondant au message TEMM, contenant notamment le résultat du chiffrement par la clé 306 KpubTr de :
  - données 316 d'autorisation,
  - d'un identifiant de contenu 318 ,
  - et des droits 319 d'utilisation du contenu issus à l'origine de la licence 201.

Le dispositif 302 envoie ensuite ce paquet 340 TEMM au module 304. Les données 316 d'autorisation peuvent contenir une clé d'authentification éphémère K et une clé de chiffrement éphémère R, générées de manière aléatoire par le dispositif d'accès 302, telles que définies dans la demande de brevet publiée sous le numéro WO 02/47356 citée précédemment. Les droits 319 d'utilisation du contenu définissent les conditions d'utilisation du contenu dans le dispositif portable, par exemple « droit de voir le film deux fois ».

- étape 356 : le dispositif 302 d'accès génère aléatoirement une clé symétrique 310 K_{LECM}. Cette clé 310 K_{LECM} est ensuite chiffrée par l'intermédiaire de la clé 306 KpubTr et le résultat 311 $E\{KpubTr\}(K_{LECM})$ est envoyé au module 304,
- étape 358 : le module 304 déchiffre $E\{KpubTr\}(K_{LECM})$ grâce à la clé 312 privée KprivTr, re-chiffre K_{LECM} grâce à la clé 314 K_{DP} symétrique du dispositif portable et renvoie le résultat 324 $E\{K_{DP}\}(K_{LECM})$ de ce chiffrement au dispositif 302 d'accès,
- étape 360 : le dispositif 302 d'accès crée des paquets 322 de données correspondant aux messages TECM; ces paquets 322 TECM sont introduits dans le contenu 232 comme illustré schématiquement à la figure 3b représentant la structure 330 des données du contenu 232 (figure 2) dans l'exemple du standard DVB-MPEG2 (acronyme de l'anglais « Digital Vidéo Broadcasting Motion picture Expert Group »). Les paquets 322 TECM contiennent :
  - des données 326 comprenant le résultat 324 $E\{K_{DP}\}(K_{LECM})$,
  - des données 328 comprenant le résultat 320 du chiffrement par la clé 310 symétrique K_{LECM} d'un ensemble de données comprenant notamment :

- une clé d'embrouillage des paquets de données formant le contenu (par exemple un mot de contrôle CW),
- des données d'autorisation et
- l'identifiant de contenu 318 ;

On notera que l'identifiant de contenu 318 peut être transmis en clair dans les paquets TECM qui contiennent également, dans une partie en clair, les droits d'utilisation du contenu converti selon un format propre au domaine 200.

On notera également que, dans le cas où les données d'autorisation 316 incluses dans le paquet 340 TEMM contiennent une clé d'authentification éphémère K et une clé de chiffrement éphémère R générées de manière aléatoire par le dispositif d'accès 302, ces clés sont utilisées comme suit dans les paquets 322 TECM : la clé de chiffrement éphémère R est utilisée pour « sur-chiffrer » la clé d'embrouillage des paquets formant le contenu et la clé éphémère d'authentification K correspond aux données d'autorisation. Ainsi, selon cet exemple particulier, chaque paquet 322 TECM contient :

$E\{K_{DP}\}(K_{LECM}) \mid E\{K_{LECM}\}(E\{R\}(CW), K, \text{identifiant}) \mid \text{droits}$

Chaque paquet 322 TECM est placé dans une cryptopériode 331 (dans le monde de l'accès conditionnel, une cryptopériode 331 correspond à une période pendant laquelle une même clé d'embrouillage CW est utilisée pour chiffrer le contenu – elle a généralement une durée d'environ 10 secondes) avec un ensemble de paquets 332 transportant des parties du contenu 232, puis le dispositif 302 envoie les paquets 322 TECM insérés dans le contenu 330 au module 304.

Une fois que le contenu 232 a été transféré au dispositif 212 (avec les paquets 322 TECM), le contenu 232 est ré-utilisable en cas d'acquisition de nouveaux droits (par exemple, acquisition des droits correspondants à une consommation supplémentaire), pour être consommé soit au niveau du dispositif 212 isolé portable, soit dans tout autre dispositif pouvant consommer des contenus gérés par le dispositif 212 isolé portable.

Suite à l'étape de transfert du dispositif 206 d'accès vers le dispositif 212 portable d'un contenu 232 isolé avec la licence 234 isolée associée (figure 2), la consommation du contenu 232 peut se produire :

- soit dans le dispositif 212 portable lui-même si ce dispositif 212 contient des moyens nécessaires pour réaliser cette consommation (tels que écran d'affichage, haut-parleurs ou prise pour écouteurs). Les étapes suivantes sont alors mises en œuvre :
  - le module 230 contrôle que la consommation peut être réalisée dans le cadre des droits acquis dans la licence 234 (si ce n'est pas le cas, la consommation est alors refusée),
  - le module 230 met à jour les droits d'utilisation du contenu dans la licence 234, puis
  - le module 230 envoie une autorisation de consommation aux moyens de consommation propres au dispositif 212 isolé portable.
- soit au niveau d'un autre dispositif du domaine 200 pouvant se connecter temporairement au dispositif 212, notamment un dispositif de la partie 211 isolée du domaine 200, dénommé dispositif de présentation du contenu. Les étapes suivantes sont alors mises en œuvre:
  - le dispositif 212 portable se connecte à un ou plusieurs dispositifs du domaine 200,
  - le dispositif portable 212 diffuse le contenu 232 aux dispositifs du domaine 200 auxquels il est connecté,
  - un dispositif de présentation (par exemple la télévision 218 de la résidence secondaire 216) demande l'autorisation de consommer le contenu 232 au dispositif 212 (c'est à dire dans le cas de la télévision 218, le droit de l'afficher sur son écran),
  - le module de gestion 230 du dispositif portable 212 vérifie alors les droits dans la licence 234 et, si la demande peut être acceptée, il met à jour la licence 234 et envoie l'autorisation et le contenu au dispositif de présentation.

Dans un mode de réalisation préféré où les données d'autorisation sont celles utilisées dans la demande de brevet publiée sous le numéro WO 02/47356 citée précédemment décrivant un protocole dans lequel on autorise uniquement une consommation directe du contenu sans droit de copie (« view

only »), le procédé de consommation du contenu au niveau d'un dispositif de présentation 218, 222 (figure 2) se déroule comme suit.

Tout d'abord, un processus similaire à celui qui a été décrit en liaison avec la figure 3 se déroule entre le dispositif de présentation (qui joue le rôle du module de gestion 304 de la figure 3 et qui contient la clé K_N propre au domaine 200) et le dispositif 212 isolé portable (qui joue le rôle du dispositif d'accès 302 de la figure 3) à l'issu duquel le dispositif 212 peut remplacer les paquets TECM du contenu par des paquets LECM qui contiennent la clé symétrique K_{LECM} chiffrée avec la clé K_N du domaine (et non avec la clé K_{DP} du dispositif 212 comme dans les TECM). Les paquets LECM sont ensuite envoyés au dispositif de présentation avec le contenu.

Le dispositif de présentation déchiffre alors les paquets LECM à l'aide de sa clé K_N. Il obtient ainsi la clé éphémère d'authentification K ainsi que les clés d'embrouillage CW du contenu qui sont chiffrées à l'aide de la clé éphémère de chiffrement R. Il génère alors un aléa Ri qu'il envoie au dispositif portable 212.

Le dispositif 212 calcule une données d'authentification $MAC_K(Ri)$ (« MAC » signifiant « Message Authentication Code ») à partir de cet aléa Ri et de la clé d'authentification éphémère K. Il faut ici noter que le dispositif 212 récupère cette clé K ainsi que la clé R du paquet TEMM (qui constitue une partie de la licence 234) en déchiffrant les données d'autorisation de ce paquet TEMM à l'aide de sa clé privée KprivTr. Il envoie ensuite au dispositif de présentation la clé éphémère de chiffrement R et la donnée d'authentification $MAC_K(Ri)$.

Le dispositif de présentation peut ensuite vérifier la donnée d'authentification reçue à l'aide de la clé K et ainsi vérifier que le contenu provient bien d'une source autorisée. A l'aide de la clé R, il peut ensuite déchiffrer les clés d'embrouillage du contenu et désembrouiller le contenu.

Cette invention est susceptible de nombreuses variantes.

Le dispositif 212 isolé portable peut être aussi le dispositif 206 d'accès. Il n'est pas nécessaire à l'invention de personnaliser le contenu 203 et la licence 201 en contenu 224 et licence 226, le contenu 203 et la licence 201 peuvent être directement adaptés en contenu 232 et en licence 234.

Aussi, la clé 314 symétrique comprise dans le module 304 du

dispositif 212 isolé portable peut être la même qu'une clé symétrique utilisée pour la consommation du contenu dans la partie 207 du réseau à partir du dispositif 206 d'accès.

Le module 230 peut être réalisé par d'autres moyens qu'une carte à puce pour stocker et traiter des informations de chiffrement, comme par exemple un processeur sécurisé ou un processeur associé à des logiciels anti-fraude.

Le dispositif 212 portable peut être notamment un baladeur audio ou vidéo, un téléphone mobile, un dispositif électronique de gestion de données personnelles (PDA, en anglais 'Personal Digital Assistant') ou un dispositif de stockage de données équipé de moyens de traitement cryptographique.

REVENDICATIONS

1. Procédé de protection d'un contenu (201) fournisseur audio et/ou vidéo d'un fournisseur (202(i)) dans un domaine (200) client comprenant un dispositif (212) isolé portable, caractérisé en ce que:

a. le dispositif (212) isolé portable reçoit un contenu (232, 330) isolé, résultat d'un traitement numérique du contenu (201) fournisseur audio et/ou vidéo, et une licence (234) isolée associée au contenu et contenant des droits d'utilisation du contenu (232, 330) isolé et des informations d'autorisation,

b. le dispositif (212) isolé portable gère la consommation du contenu (232, 330) conformément aux droits associés qu'il a reçu dans des dispositifs du domaine (200), indépendamment du fournisseur (202(i)).

2. Procédé selon la revendication 1, caractérisé en ce que le dispositif (212) isolé portable se connecte à un dispositif (206, 302) d'accès temporairement en vue d'acquérir le contenu (232, 330) isolé et la licence (234) isolée contenant les droits d'utilisation du contenu (232, 330) isolé et les informations d'autorisation.

3. Procédé selon la revendication 2, caractérisé en ce que le dispositif (206, 302) d'accès crée un paquet (340) de données de gestion des droits d'utilisation du contenu, dénommé TEMM, contenant notamment le résultat d'un chiffrement, déchiffrable par le dispositif (212) isolé portable:

- de données (316) d'autorisation,
- d'un identifiant de contenu (318),
- de droits (319) d'utilisation du contenu,

et envoie ce paquet (340) TEMM au dispositif (212) isolé portable.

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que le dispositif (206, 302) d'accès crée des paquets (322) de données de contrôle, dénommés TECM, qui sont envoyés au dispositif (212) isolé portable introduits dans le contenu (232, 330) isolé et qui contiennent :

- un ensemble (320) chiffré de données comprenant :

- une clé d'embrouillage des paquets de données formant le contenu, et
- des données d'autorisation, et

- des informations (324) sur le chiffrement permettant au dispositif (212) isolé portable de déchiffrer l'ensemble (320) de façon sécurisée.

5. Procédé selon la revendication 4, caractérisé en ce que la clé d'embrouillage contenue dans le paquet de données de contrôle est en outre protégée par une donnée d'autorisation.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que les droits associés au contenu (201) fournisseur dans le dispositif (206, 302) d'accès sont mis à jour en soustrayant les droits envoyés au dispositif (212) isolé portable.

7. Procédé selon la revendication 1, caractérisé en ce que le contenu (232, 330) est consommé au niveau du dispositif (212) isolé portable.

8. Procédé selon la revendication 1 ou 7, caractérisé en ce que les moyens (230, 304) de gestion envoient l'autorisation de consommation aux moyens de consommation propres au dispositif (212) isolé portable et mettent à jour les droits compris dans la licence (234) isolée au fur et à mesure de la consommation du contenu (232, 330) dans le dispositif (212) isolé portable.

9. Procédé selon la revendication 1, caractérisé en ce qu'un dispositif (210, 208, 222, 218) ayant des moyens de consommation de contenus, dénommé dispositif (210, 208, 222, 218) de présentation, se connecte au dispositif (212) isolé portable temporairement.

10. Procédé selon la revendication 9, caractérisé en ce que, lorsque le dispositif (210, 208, 222, 218) de présentation demande l'autorisation d'acquérir le contenu (234, 330) pour le consommer au dispositif (212) isolé portable, les moyens (230) de gestion du dispositif (212) isolé portable vérifient la présence des droits demandés par le dispositif (210, 208, 22, 218) de présentation dans la licence (234) isolée et, si la demande d'autorisation est justifiée, la mettent à jour et envoient l'autorisation et le contenu (234, 330) au dispositif (210, 208, 22, 218) de présentation pour y être consommé.

11. Procédé selon la revendication 1, 9, 10 ou 11, caractérisé en ce que le dispositif (218, 222) de présentation appartient au domaine (200) client.

12. Dispositif (212) isolé portable, caractérisé en ce qu'il contient des moyens (230) de gestion pour mettre en œuvre le procédé selon l'une des revendications précédentes.

13. Dispositif (206, 302) d'accès, caractérisé en ce qu'il comprend des moyens pour mettre en œuvre le procédé selon l'une des revendications 1 à 11.

1/4

FIG_1

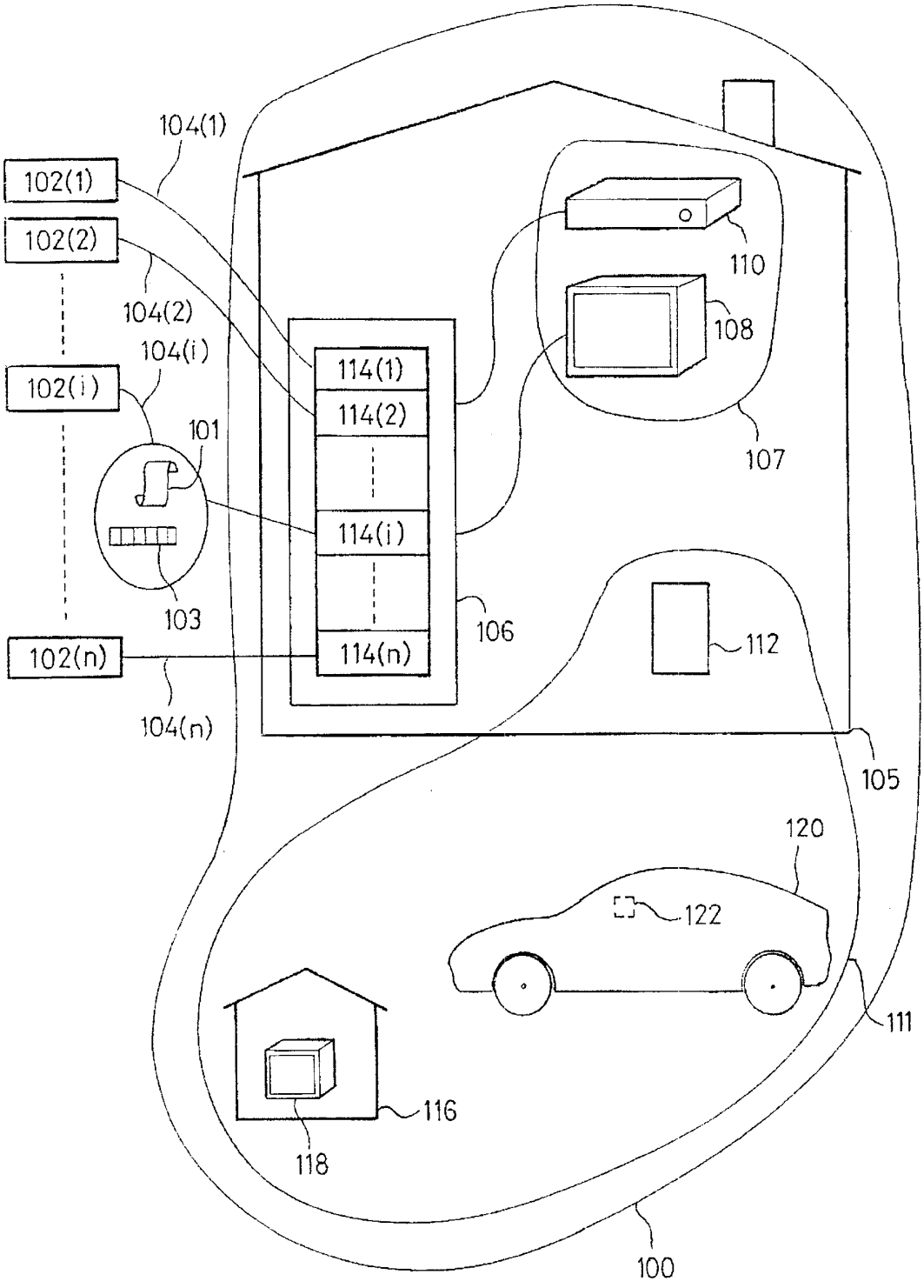

104(1)
102(1)
102(2)
104(2)
104(i)
102(i)
101
103
102(n)
104(n)
114(1)
114(2)
114(i)
114(n)
106
110
108
107
112
105
120
122
111
116
118
100

FIG_2

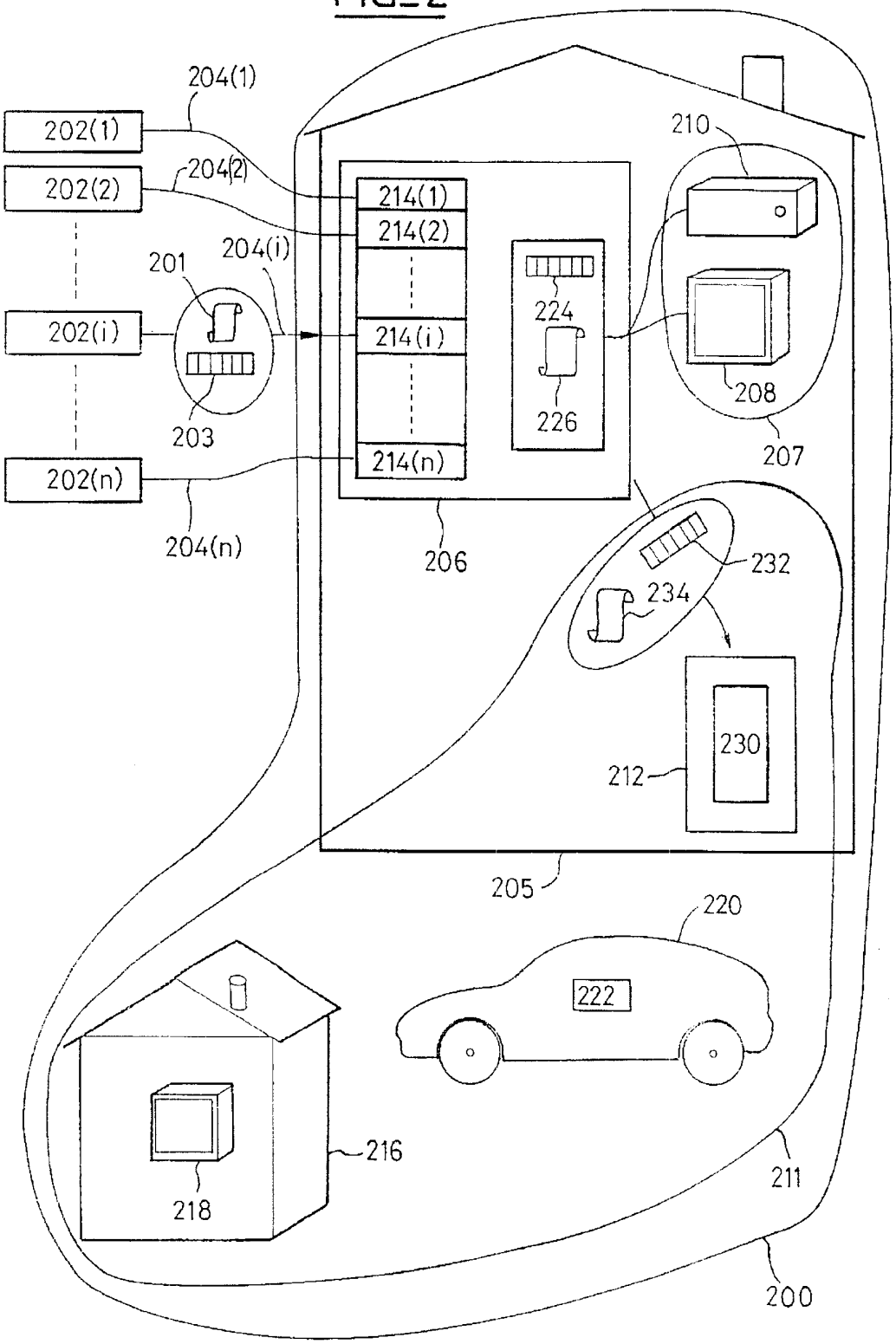

204(1)
202(1)
202(2)
204(2)
214(1)
214(2)
210
201
204(i)
202(i)
214(i)
224
226
208
203
214(n)
207
202(n)
204(n)
206
232
234
230
212
205
220
222
216
218
211
200

FIG_3

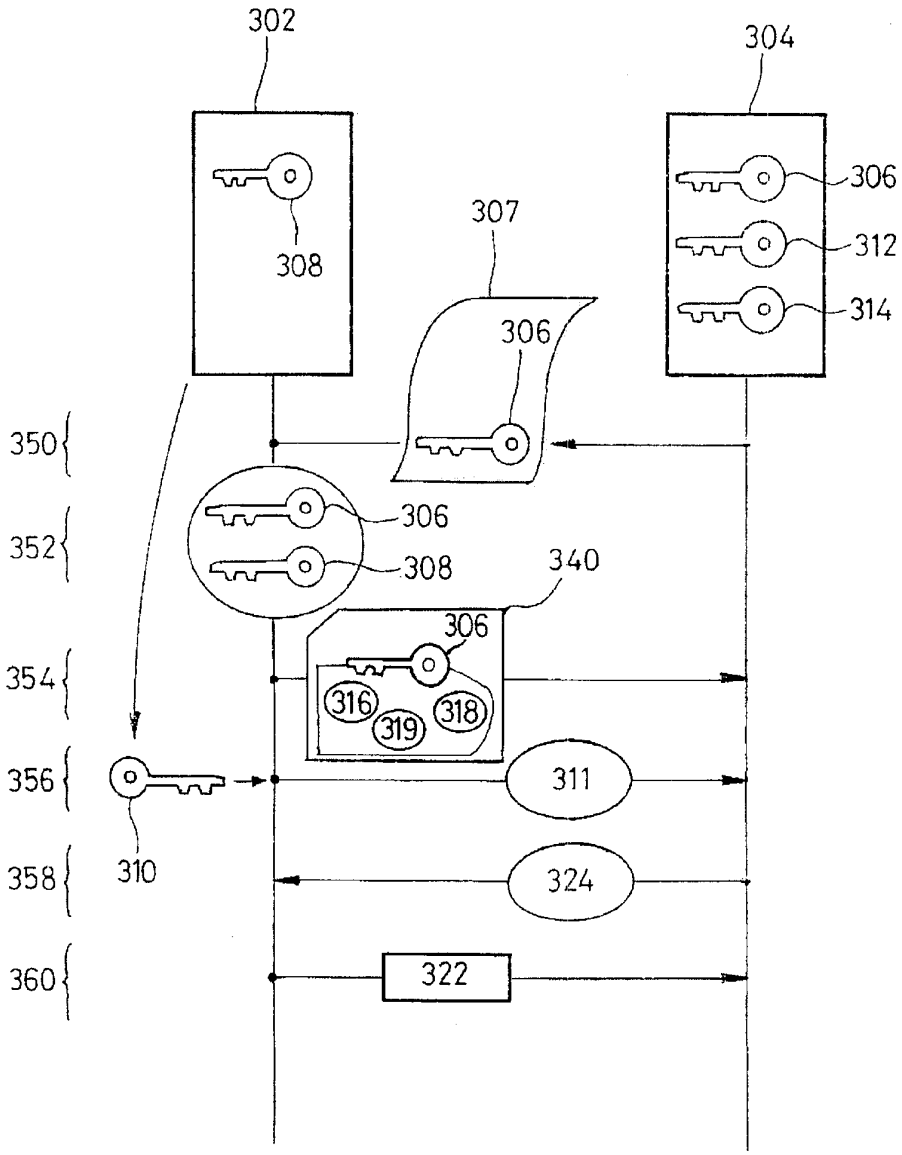
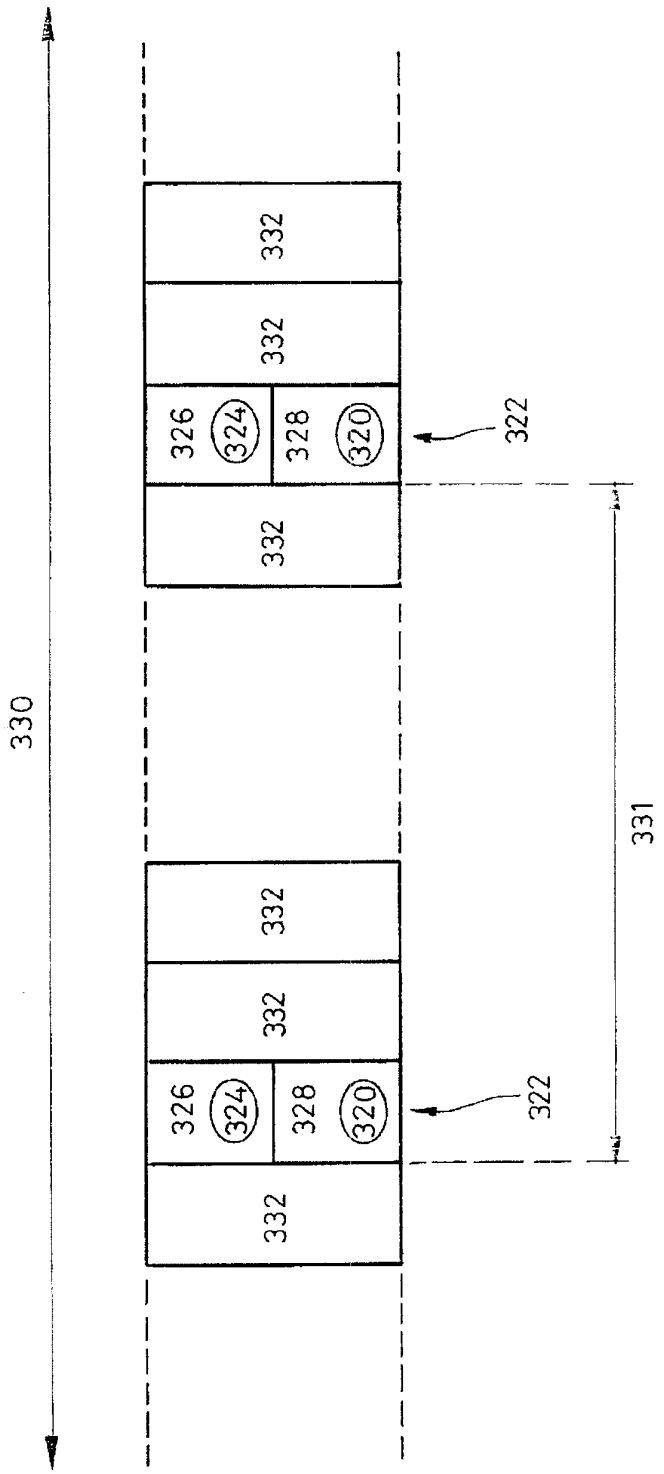

302
304
306
308
307
312
314
306
350
352
306
308
340
306
354
316
319
318
356
311
310
358
324
360
322

FIG_4



RÉPUBLIQUE FRANÇAISE

2881596

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 659438
FR 0550254

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	EP 1 271 279 A (MICROSOFT CORPORATION) 2 janvier 2003 (2003-01-02) * alinéas [0151] - [0157] * * alinéas [0162] - [0173] *	1-13	H04L12/22 H04L9/30
A	WO 03/005174 A (NOKIA CORPORATION) 16 janvier 2003 (2003-01-16) * alinéas [0007] - [0010], [0019], [0034], [0037], [0038] *	1-13	
A	US 2002/157002 A1 (MESSERGES THOMAS S ET AL) 24 octobre 2002 (2002-10-24) * alinéas [0010], [0028], [0032], [0036], [0038], [0060], [0061] *	1-13	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04L G06F

Date d'achèvement de la recherche	Examinateur
11 octobre 2005	Lázaro, M.L.

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0550254 FA 659438

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 11-10-2005
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1271279 A	02-01-2003	JP 2003101526 A	04-04-2003
WO 03005174 A	16-01-2003	EP 1412833 A1	28-04-2004
US 2002157002 A1	24-10-2002	CN 1503944 A	09-06-2004
		EP 1390851 A1	25-02-2004
		JP 2004535623 T	25-11-2004
		WO 02086725 A1	31-10-2002

EPO FORM P0465